REMARKS

This is in response to the Office Action dated September 15, 2009, in which claims 36-62 were rejected. Claims 1-35 were previously cancelled. With this Amendment, claim 40 has been cancelled and claim 63 has been added as a new claim in the application. No new matter has been introduced as a result of the addition of claim 63. Applicant respectfully requests consideration and allowance of all pending claims.

I. CLAIM REJECTIONS – 35 USC § 103

Claims 36-62 were rejected under 35 U.S.C. 103(a) as being unpatentable over Moharram, et al., U.S. Patent No. 7,290,286 in view of Immonen, U.S. Patent No. 6,931,528.

Claim 36 includes:

- generating a first shared secret key for the second peer with the first public key of the first certificate; and
- generating a second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer.

Column 3, lines 16-27, of Immonen, a portion of which is cited in the Office Action, is as follows:

> In step 25, B verifies C_A, obtains A's public key E_A and calculates the shared secret key. In step 26, B sends a second inter-party message to A. The second inter-party message comprises B's certificate C_B. It also indicates that B has been able to verify A's certificate. (However, this indication can be an implicit one, meaning that B only sends its certificate if it has verified A's certificate.) In step 27, A verifies B's certificate C_B, obtains B's public key E_B and calculates the shared secret key. In step 28, A sends B a third inter-party message comprising a finished message which indicates that it has been able to verify B's certificate.

As noted above, independent claim 36 includes "generating a first shared secret key for the second peer with the first public key of the first certificate." While the above-included section of Immonen describes "verifying a certificate," "obtaining a public key" and "calculating a shared secret key," there is nothing in Immonen about generating a shared secret key with a

public key of a certificate. Further, Immonen appears to utilize an identical method to calculate shared secret keys for both peers. However, as noted above, claim 1 features "generating a first shared secret key for the second peer with the first public key of the first certificate; and generating a second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer." Moharram also appears to use an identical method to calculate shared secret keys for two peers. Further, Moharram includes nothing about "generating a first shared secret key for the second peer with the first public key of the first certificate." Thus, the combination of Immonen and Moharram does not teach or expressly or impliedly suggest all the elements of claim 36.

In view of the foregoing, claim 36 is believed to be allowable over the cited art. Independent claims 51 and 57 have elements similar to those of independent claim 36. Thus, for the same reasons as independent claim 36, Applicant submits that independent claims 51 and 57 are allowable as well. Applicant respectfully submits that the dependent claims are also allowable by virtue of their dependency, either directly or indirectly from the allowable independent claims. Further, the dependent claims set forth numerous elements not shown or suggested in the prior art.

Claim 63 has been added as a new claim in the application. In addition to the limitations of claim 36, new claim 63 includes that "generating the first shared secret key for the second peer with the first public key of the first certificate is carried out independently of any public key generated by the first peer and the second peer."

Immonen includes nothing about the above element of claim 63. Further, column 3, lines 43-46, of Immonen are as follows:

> Suitable key exchange algorithms include Diffie-Hellman (DH) with fixed parameters certified with Digital Signature Algorithm (DSA). The DH algorithm can be found in most textbooks on cryptography.

Page 16, lines 3-12, of the specification are as follows:

> In the case where the client has a certificate containing fixed DH parameters, the certificate contains the information required to complete the key exchange and the client and server

> will generate the same DH result. In the case where the client has a standard DSS certificate, it sends a set of temporary parameters to the server in the client key exchange message, then optionally uses the certificate to verify a message to authenticate itself. The present invention does not use the DH parameters but the DSS parameters. In addition, the present invention also uses the certificate public key to obtain the shared secret key at the server. This way, one exponentiation operation is eliminated since a Diffie-Hellman public key from the client is not needed to obtain the shared secret key at the server.

By including "generating the first shared secret key for the second peer with the first public key of the first certificate is carried out independently of any public key generated by the first peer and the second peer," claim 63 is saving a step of the Diffie-Hellman algorithm, which is in contrast with the above teachings of Immonen, which recommends the use of the Diffie-Hellman algorithm. Moharram does not make up for the deficiencies of Immonen. Thus, new claim 63 is believed to be allowable.

In view of the foregoing, Applicants respectfully request reconsideration and allowance of claims 36-39 and 41-63. Favorable action upon all claims is solicited.

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: /Alan G. Rego/

Alan G. Rego, Reg. No. 45,956
900 Second Avenue South, Suite 1400
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

AGR:dmm